UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/733,912	12/12/2000	Yuji Seki	108392-00000	5483

7590 12/16/2004

ARENT FOX KINTNER PLOTKIN
& KAHN, PLLC
Suite 600
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5339

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/733,912	SEKI ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/19/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on October 19, 2004.

Begin FAOM Dated 05/03/2004

This action is in response to the communication filed on December 12, 2000.

DETAILED ACTION

1. Claims 1-11 have been examined.

Title

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

3. The following title is suggested: *Secure Encryption Processor with Authentication and Tamper Protection*

Priority

4. This application claims foreign priority, under Title 35 U.S.C. 119 (a-d), to Japanese Application 196040/2000.

5. The effective filing date of the subject matter defined in the pending claims of this application is 06/29/2000.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 12/12/2000 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The drawings filed on July 31, 2000 are objected to because:

Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

Figure 2 Element 211 should be labeled "SSL Message" in order to obtain consistency with the rest of the figure.

Figure 7 Element 4060 is not entirely consistent with page 35 lines 17-19. The examiner suggests that the figure is redrawn to more clearly show the path of 4060 reaching 4000.

Figures 7 and 8 are incomplete because the tops of these figures are above the required top margin and therefore have been altered by the hole-punch.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

7. The abstract of the disclosure is objected to under Title 37 CFR 1.72 because of the following informalities:

The phrase "encryption control apparatus" of line 3 repeats information in the title and therefore must be removed accordingly.

The phrase "is provided" of line 5 can be implied and therefore must be removed.

8. The Brief Description of the Drawings is objected to under Title 37 CFR 1.74 because the brief descriptions of figures 8 and 9 do not describe the contents of the figures.

Correction is required. See MPEP § 608.01(b).

9. The examiner advises the applicant to carefully review the disclosure to ensure that there are no grammatical, spelling or other errors that the examiner may have missed, and to correct any error that may be found.

Claim Objections

10. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

11. Claim 11 objected to because of the following grammatical error:

Lines 2-3 recite "data destroying means for; upon receipt of abnormality detection, destroying a key stored in RAM." The examiner suggests "data destroying means, which upon receipt of an abnormality, destroys a key in RAM" be used instead.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 2, 3, and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

14. Claim 2 Lines 8 and 11, claim 3 Line 8, and claim 6 line 3 recite "external". Because the word "external" is an adjective, it must modify a noun. "External" as used in claims 2 and 6 does not modify a noun and therefore renders the claim indefinite. This is because one of ordinary skill in the art could not determine what the applicant considers "an external". For purposes of searching prior art, the examiner will assume that the applicant means "external source" in claim number 2 and "external destination" in claim number 6.

Claim Rejections - 35 USC § 102

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

16. Claims 1-4, 7-9 rejected under 35 U.S.C. 102(b) as being anticipated by Abraham et al. (U.S. Patent 5,048,085) hereinafter referred to as Abraham.

17. Regarding claim 1, Abraham disclosed a microprocessor (element 71), ROM (element 75), RAM (element 73), I/O gates (element 87), and an encryption processor (element 85), all on a single semiconductor device (See Abraham Fig. 3).

18. Regarding claim 2, Abraham disclosed storing keys in RAM (See Abraham Col 6 Lines 64-65), storing authorization profiles (See Abraham Col. 9 Lines 15-22), and command authentication based on user profile in which a wait mode is used when the adapter is not in use (See Abraham Fig. 7).

19. Regarding claim 3, Abraham disclosed multiple commands (See Abraham Fig. 12) that can be run based on command requests from the user (See Abraham Fig. 7).

20. Regarding claim 4, Abraham disclosed a signature verification section used to authenticate a user (See Abraham Fig. 4 Elements 101 and 103 and Fig. 14 Elements 335-341).

21. Regarding claim 7, Abraham disclosed storing the keys in RAM (See Abraham Col. 6 Lines 64-65), storing authorization profiles (See Abraham Col. 9 Lines 15-22), and user verification in order to process commands (See Abraham Fig. 9) of which I/O commands are included (See Abraham Fig. 12).

22. Regarding claim 8, Abraham disclosed multiple I/O sections, including a card reader, an operator interface, a pen interface, and an ASYNC RS232 interface (See Abraham Fig. 3). Abraham also disclosed user verification in order to process commands (See Abraham Fig. 9) of which I/O commands are included (See Abraham Fig. 12).

23. Regarding claim 9, Abraham disclosed unsecured and secured sessions depending on the command being executed (See Abraham Fig. 9 Element 209). Abraham further disclosed establishing secure sessions with other devices (See Abraham Col. 3 Lines 53-65).

24. Claims 1, 5-6 rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan (U.S. Patent 5,737,419) hereinafter referred to as Ganesan.

25. Regarding claim 1, Ganesan disclosed a processor (Element 700), ROM (Element 722), RAM (Element 720), I/O (Elements 726, 728, 729, 730, 740, and 760) (See Ganesan Fig. 6). Ganesan also disclosed encrypting and decrypting messages (See Ganesan Abstract).

26. Regarding claim 5, Ganesan disclosed generating encryption keys (See Ganesan Abstract).

27. Regarding claim 6, Ganesan disclosed the use of asymmetric keys, particularly public and private keys (See Ganesan Abstract). Ganesan also disclosed storing keys in RAM (See Ganesan Col. 19 Paragraph 4).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

29. Claim 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham as applied to claim 1 above, and further in view of Kashkashian, Jr. (U.S. Patent 4,700,055) hereinafter referred to as Kashkashian.

Abraham disclosed communication with a network security processor (See Abraham Fig. 15 Elements 351-357). However, Abraham failed to disclose the use of a modem for this communication.

Kashkashian teaches that authorization can be performed on a remote computer by communicating necessary information between the local and remote computers via a modem (See Kashkashian Col. 4 Lines 33-49).

It would have been obvious to one skilled in the art at the time of invention to employ the teachings of Kashkashian to the invention of Abraham in order to communicate the between the cryptographic adapter and the network security processor. This would have been obvious because one skilled in the art would have been motivated to communicate between the local adapter and the remote network security processor.

30. Claim 11 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham as applied to claim 1 above, and further in view of Double et al. (U.S. Patent 5,027,397) hereinafter referred to as Double.

Abraham disclosed a tamper protection circuit according to U.S. Patent number 5,027,397 (See Abraham Col. 6 Line 67 – Col. 7 Line 6). Abraham further disclosed this circuit being connected to the RAM holding the cryptographic keys (See Abraham Fig. 3 Elements 73 and 81). However, Abraham failed to disclose the tamper protection circuit destroying the cryptographic keys.

Double teaches that in order to protect cryptographic keys stored in volatile memory, one can employ a tamper protection circuit that will erase the volatile memory and the keys when an attack is detected (See Double Description of the preferred embodiment).

It would have been obvious to a person of ordinary skill in the art at the time of invention to employ the teachings of Double as the tamper protection circuit of the Cryptographic Adapter of Abraham in order to delete cryptographic keys stored in RAM in the event of a security attack. This modification would have been obvious because one skilled in the art would have been motivated to protect the private cryptographic keys from unauthorized access and use.

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Esserman et al. (U.S. Patent 5,111,504) disclosed a replaceable security element.

b. Eyer et al. (U.S. Patent 5,134,700) disclosed a microcomputer with internal RAM security during external program mode.

c. Abraham et al. (U.S. Patent 5,148,481) disclosed a transaction system security apparatus.

d. Double et al. (U.S. Patent 5,159,629) disclosed a tamper detection and protection circuit.

e. Abraham et al. (U.S. Patent 5,301,231) disclosed a user defined function facility to provide flexible cryptographic processing.

f. Ishii (U.S. Patent 5,768,389) disclosed generation and management of a secret key in a public key cryptosystem.

g. Walker et al. (U.S. Patent 5,794,207) disclosed a cryptographically assisted commercial network system.

h. Collins et al. (U.S. Patent 6,378,072) disclosed a public key cryptosystem.

End FAOM Dated 05/03/2004

Response to Amendment

32. All rejections and objections, not set forth below have been withdrawn.

33. The information disclosure statement (IDS) submitted on 10/19/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

34. The examiner withdraws all objections to the drawings presented in the FAOM dated 05/03/2004. As noted in the applicant's response, the examiner was considering drawings for a different case. As, such, the drawings submitted on 12/12/2000 are acceptable for examination proceedings.

35. The examiner maintains the rejection of claim 1, as being anticipated by Abraham, as set forth in the FAOM dated 05/03/2004. The applicant traverses primarily that Abraham did not disclose that the RAM, ROM, microprocessor, I/O gates, and encryption processor were not all formed on a single semiconductor device. Abraham clearly depicted that the cryptographic module (Element 31), which contained the elements of claim 1, was formed on a PCI card or the

like (See Abraham Fig. 1 Element 29). Microsoft Computer Dictionary, regarding *semiconductor,* states that "the term is used loosely to refer to electronic components made from semiconductor materials." As can be seen from Abraham Fig. 4, the cryptographic adapter card was clearly an electronic component made from semiconductor materials, including elements 83, and 91-103. Also, Fig. 4 clearly depicts the card being a single device. Therefore, the cryptographic module, element 31, was formed on a single semiconductor device.

36. The examiner maintains the rejections of claims 2-4, and 7-11, as presented in the FAOM dated 05/03/2004.

37. The examiner maintains the rejection of claim 1, as being anticipated by Ganesan, as set forth in the FAOM dated 05/03/2004. The applicant traverses primarily that Ganesan did not disclose that the processor, ROM, RAM, and I/O were not formed on a single semiconductor device. As can be seen in Fig. 7, Ganesan clearly depicted the elements listed in claim 1, as being inside a computer all formed in connection with bus 710. It is well known that in a computer, processors, ROM, RAM, I/O and the bus are all formed on a motherboard. As is also well known in the art, a motherboard is an electronic component made from semiconductor materials, including diodes, transistors, capacitors, etc. Therefore, a motherboard is a single semiconductor device. As such, although it was not specifically disclosed by Ganesan that the components were formed on a motherboard, it was inherent that the processor, ROM, RAM, I/O, and bus were formed on a motherboard. Therefore, they were formed on a single semiconductor device.

38. The examiner maintains the rejections of claims 5-6, as presented in the FAOM dated 05/03/2004.

39. Claims 1-11 have been finally rejected.

40. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

41. Any inquiry concerning this communication should be directed to Matthew Henning whose telephone number is (703) 305-0713. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131
12/10/2004

EMMANUEL L. MOISE
PRIMARY EXAMINER